Arctic Wolf Risk Assessment Solutions

Continuous Risk Assessment, Made Simple

Risk assessment solutions in the Arctic Wolf RootSecure portfolio constantly probe your network, monitor your connected devices, and test your organization's social engineering resilience. They provide a quantified, real-time view into your cyber risks and let you focus your actions where they're needed.

The Arctic Wolf Risk Assessment Difference

Arctic Wolf RootSecure Dashboard

The RootSecure Dashboard is tailored to your organization's priorities to help you make sense of your organization's network, devices, and people vulnerabilities and help you take prioritized steps to reduce cyber risk exposure.

Comprehensive Visibility into Your Risk Posture

- **Dynamic Asset Identification:** Automatic and continuous profiling and classification of your network assets to build a comprehensive inventory
- **Continuous Risk Scanning:** Ongoing scans rather than occasional ones to avoid risky delays in security awareness
- **Comprehensive Risk Profiling:** Aggregates and quantifies risk indicators from RootSecure products, which are weighted based on the industry standard CVSS (Common Vulnerability Scoring System)
- **External/Internal Network Scanning:** identifies vulnerabilities that could be exploited in internet-facing and internal systems on the network; Host-Based Risk Assessment: Host-based agents monitor hardware and software, and registry configurations and changes to reveal risks that can only be detected through on-device observations
- **Social Engineering Simulation:** Puts your people to the test and quantifies how vulnerable your organization is to social engineering attacks, both broad and targeted

AWN RootSecure Portfolio

Arctic Wolf RootSecure risk assessment products —Reach, Scout, and Echo—continuously test your networks, devices, and people, respectively, looking for vulnerabilities and securely reporting the findings to the RootSecure Dashboard.

RootSecure Reach

Continuous Network Scanner

External and internal vulnerability assessment tools that discover IP-connected devices, look for vulnerabilities resulting from outdated software, and prioritize your patch strategy.

- **Reach eVA:** scans internet-facing servers to understand your company's digital footprint. Key features include:
  - Continuous scanning of external-facing assets
  - Proactive risk monitoring
  - Webserver scans
  - Automated sub-domain detection
  - Darkweb scans
- **Reach iVA:** continuously scans all your internal IP-connected devices, cataloging your core infrastructure, equipment/peripherals, workstations, internet of things (IoT) and personal (i.e., BYOD) devices. Key features include:
  - Continuous scanning of internal assets
  - Dynamic asset identification and classification
  - Webserver scans
  - Automatic updates
  - Stateless scanning and secure transfers

RootSecure Scout

Continuous Host-Based Risk Assessment

A turnkey social engineering simulator that tests the cyber hygiene of your employees and measures your organization's susceptibility to phishing emails, SMS messages, and voice calls. Key features include:

- Agent-based – Windows server/workstation, MacOS
- Proactive risk monitoring
- Audit reporting

RootSecure Echo

Social Engineering Simulation

Extends visibility inside devices, with continuous host-based monitoring to reveal threats and user behavior that put your organization at risk. With Scout, you gain authoritative, first-hand knowledge of exactly what is happening on your devices. Key features include: .

- People risk score
- Email, SMS, and voice phishing simulator
- Crowd-sourced templates
- Intelligent landing pages

RootSecure Dashboard: Quantify Your Cyber Risk Posture

A cloud-based dashboard that provides visibility into continuous cyber risk assessment by incorporating all meaningful cyber risk indicators from your business. It identifies the highest-priority issues and alerts you to emerging risks before they evolve into real problems. The RootSecure Dashboard empowers you to take meaningful, efficient action by using these key features:.

- Comprehensive risk profiling
- Informative user interface
- Proactive notifications and alerts
- Advanced threat data analysis
- Actionable reporting
- API Integrations
- Crowd-sourced templates
- Intelligent landing pages

"RootSecure has enabled Guelph Hydro to do two things: one is to quantify where we stand on risk mitigation; the other is to expose where our holes are"

– Dan Amyot, Guelph Hydro

Guelph Hydro Electric Systems Inc.

ARCTIC WOLF

AICPA SOC

SOC2 Type II Certified

Contact us
arcticwolf.com
1.888.272.8429
ask@arcticwolf.com